



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/986,319	11/08/2001	Timothy J. Simms	16222.004	5579
23117	7590	10/04/2006	EXAMINER	
NIXON & VANDERHYE, PC 901 NORTH GLEBE ROAD, 11TH FLOOR ARLINGTON, VA 22203			ABRISHAMKAR, KAVEH	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 10/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/986,319	SIMMS, TIMOTHY J.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 17 July 2006.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-3 and 5-9 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-3, and 5-9 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 17, 2006 has been entered.
2. Claims 10-153 are cancelled.
3. Claims 1-3, and 5-9 are currently being considered.

Claim Objections

4. Claim 5 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 5 repeats, in part, what is claimed in the fifth limitation of claim 1, and therefore, does not further limit the claim.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-3, and 5-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 states that a first message is transmitted **from the called party** to the calling party, said first message including "said first random number." However, in the first limitation of claim 1, the first random number is associated with the **calling party**. Therefore, it is interpreted that the calling party is the party, which has possession of the first random number. The claim is deemed indefinite because it is unclear why the called party would send the first random number to the calling party when the calling party already has possession of the first random number. The same arguments follow for the limitation concerning the second message, as the calling party is sending the second random number to the called party. For the purposes of examination, it is interpreted that the calling and called parties have the second and first random keys, respectively.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-2, 5 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (U.S. Patent 6,487,660), in view of Bellovin et al. (U.S. Patent 5,241,599).

Regarding claim 1, Vanstone discloses:

A method for establishing secure communication between a calling party and a called party, consisting essentially of:

identifying a first shared random number associated with a calling party (column 3 lines 35-42), wherein x is the first random number;

identifying a second random number associated with a called party (column 3 lines 42-44), wherein y is the second random number;

identifying said calling party to said called party (column 3 lines 45-53), wherein an identification string is sent from the ATM to the server;

generating a public-private key pair by said called party (column 5 lines 1-10), wherein the server generates its private-public key pair;

transmitting a second message from said calling party to said called party, said second message including said second shared random number, and said second message (column 3 lines 55-56) and

obtaining a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 6 lines 25-30).

Vanstone does not explicitly disclose transmitting a first message from the called party to the calling party wherein the first message includes a first random number and the public portion of the public-private key pair. Bellovin discloses a system of bi-directional secure communication where a public key is sent from a sender to a receiver, the public key being encrypted with a password (column 5 lines 18-32). Bellovin uses this exchange to set up a session key to be used for encrypting bi-directional communications between sender and receiver. Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. Bellovin transmits the public key encrypted with a password from a sender to a receiver in order to set up a session key for bi-directional communications. In Vanstone, the public keys are either built into the devices, or transmitted by a third party (column 5 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention use the method of Bellovin to transmit the public key to the calling party in order to set up a session key without the involvement of a third party which would allow the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone.

Furthermore, Vanstone does not disclose that the second message is encrypted with the public key. Bellovin discloses that a message containing a random number is encrypted with a public key (column 5 lines 33-38). Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel

between a sender and a receiver. It would have been obvious to one of ordinary skill in the art at the time of invention use a public key to encrypt the message in order to secure the exchange of the parameters so that a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Vanstone discloses:

The method of claim 1, wherein said combining function includes a logical function (column 3 lines 52-62).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Vanstone discloses:

The method of claim 1, further comprising the step of transmitting a second message from said second computer to said first computer, said second message including said second shared random number (column 3 lines 55-56).

Claim 9 is rejected as applied above in rejecting claim 5. Vanstone does not disclose wherein the first message includes an asymmetric key. Bellovin discloses a system of bi-directional secure communication where a public key is sent from a sender to a receiver, the public key being encrypted with a password (column 5 lines 18-32). Bellovin uses this exchange to set up a session key to be used for encrypting bi-

directional communications between sender and receiver. Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. Bellovin transmits the public key encrypted with a password from a sender to a receiver in order to set up a session key for bi-directional communications. In Vanstone, the public keys are either built into the devices, or transmitted by a third party (column 5 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention use the method of Bellovin to transmit the public key to the calling party in order to set up a session key without the involvement of a third party which would allow the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone.

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (U.S. Patent 6,487,660), in view of Bellovin et al. (U.S. Patent 5,241,599) in further in view of Shona et al. (U.S. Patent 6,018,581).

Claim 3 is rejected as applied above in rejecting claim 2. Vanstone-Bellovin does not explicitly disclose that the logical function is an XOR function. Shona discloses a method wherein the logical function is an exclusive-or (XOR) function (column 6 lines 12-16, lines 22-25). It would have been obvious to one of ordinary skill in the art at the

time of invention to combine the teachings of Shona with the teachings of Vanstone-Bellovin to make the encryption key greatly varied (column 6 lines 25-29).

6. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (U.S. Patent 6,487,660), in view of Bellovin et al. (U.S. Patent 5,241,599) in further in view of Wu (U.S. Patent 6,539,749).

Regarding claims 6-8, Vanstone does not explicitly disclose wherein the first message is encoded using a password. Bellovin discloses a system of bi-directional secure communication where a public key is sent from a sender to a receiver, the public key being encrypted with a password (column 5 lines 18-32). Bellovin uses this exchange to set up a session key to be used for encrypting bi-directional communications between sender and receiver. Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. Bellovin transmits the public key encrypted with a password from a sender to a receiver in order to set up a session key for bi-directional communications. In Vanstone, the public keys are either built into the devices, or transmitted by a third party (column 5 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention use the method of Bellovin to transmit the public key to the calling party in order to set up a session key without the involvement of a third party which would allow

the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone. However, the password is not encoded/encrypted. Wu teaches that the password is an encoded password (column 3 lines 33-37). Wu, Vanstone and Bellovin are all analogous arts as they are all concerned with setting up a secure communication channel via a session key. It would have been obvious to one of ordinary skill in the art at the time of invention to have combined the teachings of Vanstone-Bellovin, with the teachings of WU, in order to verify a user's asserted password without having to reveal the user's password (column 3 lines 35-37).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA
09/28/2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

Oll 9/30/06